


Havells India

IT Continuity Policy

Version 1.0

Havells India Limited Havells India IT Continuity Policy Version 1.0 Internal	
--	---

Document Control


S. No.	Type of Information	Document Data
1.	Document Title	Havells India IT Continuity Policy
2.	Document Code	HICP
3.	Date of Release	20th Feb 2023
4.	Document Superseded	
5.	Document Approvers	Mr. Pramod Mundra and Mr. Ramanand Jha
6.	Document Owner	Information Security Head
7.	Documents Author(s)	Mr. Sanjay Roongta and Mr. Neeraj Nagpal

Document Approvers

S. No.	Approver	Approver Designation	Approver Contact
1.	Pramod Mundra	Chief Information Officer (CIO)	Pramod.Mundra@havells.com
2.	Ramanand Jha	Information Security Head (ISH)	ramanand.jha@havells.com

Document Change Approvals

Version No	Revision Date	Nature of Change	Date Approved
1.0	NA	Initial Version	18th Feb 2022
1.0	NA	No Change	17th Feb 2023

Havells India Limited Havells India IT Continuity Policy Version 1.0 Internal	 HAVELLS
--	---

Document Scope

This document shall be applicable to the IT Department and the employees/Third Parties referred henceforth shall include the staff working with IT department and/or handling, processing, and managing information/information assets of Havells.

Document Distribution

The Information Security Head (ISH) shall distribute this policy to all employees working with IT department and/or handling, processing, and managing information/information assets of Havells by uploading it on the intranet/by sharing it via email/as appropriate.

Document Conventions

All statements in the document are mandatory requirements. Failure to observe these requirements may be construed as non-compliance to the policy.

Table of Contents

1. Purpose.....	5
1.1 Scope.....	5
1.2 Responsibility	5
1.3 Enforcement	5
1.4 Authority.....	5
2. IT Continuity Team	6
2.1 Roles & Responsibilities	6
3. Data Backup	7
3.1 Maintenance of IT Continuity Plan	7
4. DR detailed plan	7
4.1 SAP DR detailed plan.....	8
4.2 Infra DR detailed plan	8
4.3 Criteria for Invoking the Disaster Recovery Plan	9
5. Recovery Point Objective, Recovery Time Objective and Business Impact Analysis	10
5.1 RPO.....	10
5.2 RTO.....	10
Annexure I – RTO and RPO	10
Annexure II – BC/DR Team Telephone Numbers.....	11
Annexure III- Havells’ Head Office Escalation	12
Annexure IV- Data Centre Emergency Telephone Numbers	12
Annexure V – Disaster Recovery Centre Emergency Telephone Numbers.....	123

<p>Havells India Limited Havells India IT Continuity Policy Version 1.0 Internal</p>	
---	---

1. Purpose

In order to provide acceptable continuity of service, Havells has defined IT Continuity Policy for its IT services. The objectives of the policy are:

- a) To establish business contingency of operations of critical IT processes and deploy appropriate resources ;
- b) To train IT personnel on handling disaster recovery scenarios;
- c) To provide information to all stakeholders about the ability to continue IT operations in case of disaster.

1.1 Scope

This policy shall be applicable to the IT department and the employees/Third Party who deal with Havells' IT and/or handle, process or manage information/information assets of Havells.

1.2 Responsibility

It is the responsibility of the IT Team and respective or concerned business/functional teams to implement and maintain the guidelines as defined in the IT Continuity Policy.

1.3 Enforcement

All Employees and/or Third Party, who deal with Havells' IT and/or handle, process or manage information/information assets of Havells, must comply with this policy. All statements in the document are mandatory requirements. Failure to observe these requirements may be construed as non-compliance to the policy.

- a) Non-compliance with this policy shall be dealt with in accordance with the approved management process.
- b) Employees and Third Parties who breach this policy shall be subject to disciplinary action.

Requests for deviations from this policy must be documented and managed using the approved process. Any requests for deviations from this policy must be approved in accordance with the *Security Exception Management Policy*.

1.4 Authority

The Chief Information Officer (CIO) and Information Security Head (ISH) approves in consultation with management and enforces this policy and mandates processes to monitor and expect compliance to this Policy by respective/concerned stakeholders.

2. IT Continuity Team

2.1 Roles & Responsibilities

Below are the roles and the responsibilities for each of the personnel involved to manage a crisis-like scenario-

- Layer 1: To assess the disruption and decide to declare the event as a disaster. This shall be done by CIO / ISH.
- Layer 2: Havells' application lead, infra lead. End user support lead, solution managers and IT security lead shall be layer 2 executives. They shall be responsible for making the requisite technical infrastructure and applications available.
- Layer 3: Application support team (SAP basis/Non-SAP production support), Infra management support team (servers, data center, network, NOC operation), IT helpdesk support and SOC operations shall assist to establish communication between teams and execution of agreed set of activities as per DR Plan.

Refer: DR SOP for detailed procedures

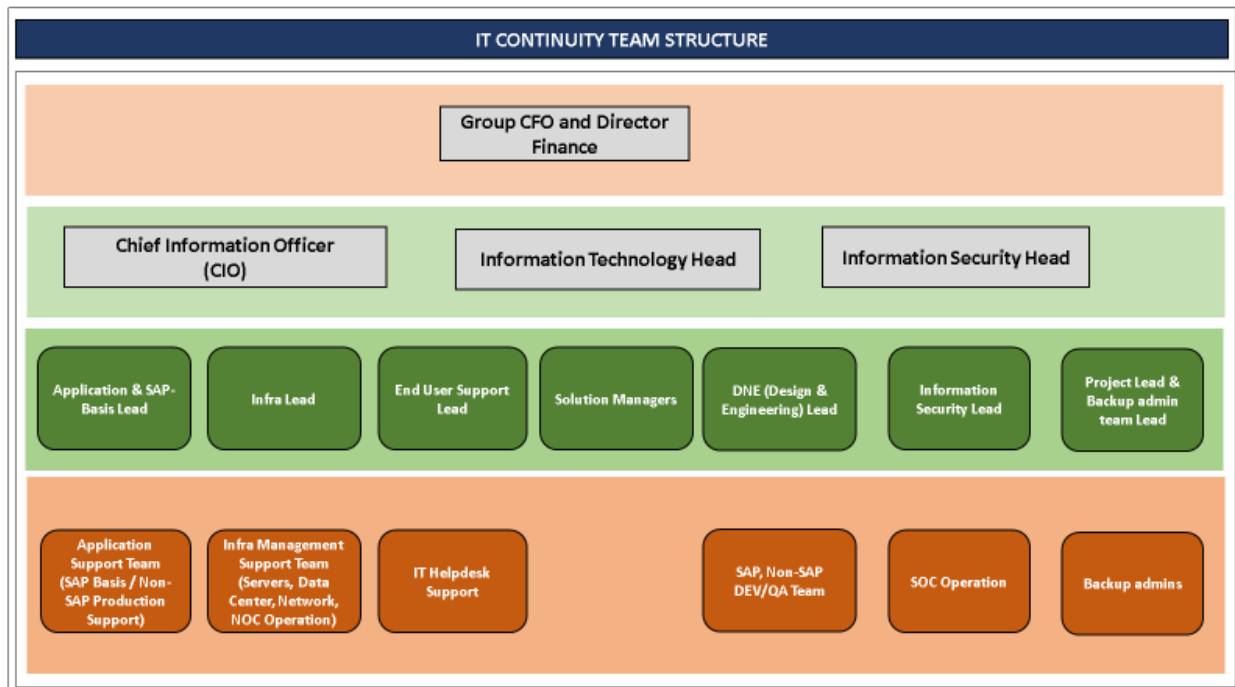


Table 1: IT continuity team

3. Data Backup

Havells has a well-defined and documented policy for taking backups of the operating system, network devices, critical applications, and databases.

Refer: Havells Backup and restoration policy

3.1 Maintenance of IT Continuity Plan

IT continuity plan shall be reviewed and updated on an annual basis. In addition, the plan shall be updated if any of the following changes but not limited to the operating environment occur:

- a) Facility changes (change to DC/DR site, change to co-location partner);
- b) Major changes to existing applications' architecture;
- c) Addition / Deletion of new applications;
- d) IT Infrastructure related changes;
- e) Adherence to backup policy / procedures; and
- f) Changes in RPO (Recovery Point Objective) / RTO (Recovery Time Objective)

3.1.1 Plan Distribution

An updated IT continuity plan shall be readily available with the following recipients:

Note: Refer to Annexure for current list of team leads. Any changes in the names of the team leads shall not require changes/modifications in the policy document.

Recipient	Location	# of Copies
CIO	Head Office	1
ISH	Head Office	1
Application & Basis support lead	Head Office	1
Basis Support lead	Head Office	1
Infra lead	Head Office	1
End user support lead	Head Office	1
Solution Manager	Head Office	1
Information security lead	Head Office	1
DNE Lead	Head Office	1
Project Lead	Head Office	1
Backup Team lead	Head Office	1

4. DR detailed plan

1. Planning and scoping
2. Vendor and required support services alignment

3. DR kick off meeting
4. Execution of IT continuity plan

Refer: DR SOP for detailed procedures

4.1 SAP and non-SAP applications DR detailed plan

1.1. Phase-1 Current State Assessment checklist and readiness

- 1.1.1. Existing SAP Application Inventory readiness for DR Setup
- 1.1.2. Existing Non-SAP application inventory readiness for DR setup
- 1.1.3. SAP & Non-SAP Application Services and modules checklist readiness
- 1.1.4. SAP & Non-SAP Application's Integration checklist
- 1.1.5. Isolated DR Test for SAP individual applications
- 1.1.6. Isolated DR test for Non-SAP individual applications

1.2. Phase-2 Integrated Testing of SAP & Non-SAP Applications for DR

- 1.2.1. Controlled DR test for integrated SAP Applications
- 1.2.2. Controlled DR test for integrated Non-SAP Applications
- 1.2.3. Overall DR testing (both SAP and Non-SAP)
- 1.2.4. Report submission
- 1.2.5. Data Sync for all SAP and Non-SAP Applications to DR setup

1.3. Phase-3 DR mock Drill UAT with Business for SAP and Non-SAP applications

- 1.3.1. Sync for all SAP and Non-SAP Applications

1.4. Phase-4 DR invoke for SAP & Non-SAP Application for Business for live transactions

1.5. Acceptance from Business for successful DR

1.6. Data replication setup from DR to DC for both SAP and Non-SAP applications(Identified approved applications)

1.7. Rollback from DR to DC as per management approval / agreed cooling period

1.8. Document lessons learnt

1.9. DR Drill -Sign-off


4.2 Infrastructure and IT Security applications DR detailed plan

1 Planning & Implementation

1.1 Phase-1 Current State Assessment

- 1.1.1 Existing Infra. Application Inventory readiness for DR Setup
- 1.1.2 Hardware/OS Inventory readiness for Infra. Application

1.2 Phase-2 DR Setup for Readiness

<p>Havells India Limited Havells India IT Continuity Policy Version 1.0 Internal</p>	
---	---

1.2.1 Application health check for available DR Application - Network (Firewall, CPPMd)

1.2.2 Firewall port detail with public & private IP - Primary DC

1.2.3 DB and Application health check for available DR Application - Security applications if any

1.2.4

1.2.5 Email gateway health check available at DR Site

1.2.6 Active Directory health check available at DR site

1.2.7 AD connect Application installation & testing at DR site

1.2.8 Confirmation on Infra. And IT Security Application's readiness

1.3 Phase-3 Invoke DR for Infra and IT Security Applications and Perform UAT inline Business requirements

1.4 Document lessons Learnt

4.3 Criteria for Invoking the Disaster Recovery Plan

Disasters that impact the service delivery of Havells' Data Centre can result in the invocation of Havells disaster recovery plan (*Refer Havells DR document*). The reporting of the event shall be done by CIO, /ISH, respective IT team Lead. This can be raised through any gadget / software/any other means. Once the event is reported, the designated authorities (for example, Building Security) have to be informed. The categorization of disaster will be done based on the following criteria:

- a) Catastrophe – Extensive damage and may have RTO (Recovery Time Objective) of more than 2 days
- b) Major – Disaster with RTO of more than 5 hours
- c) Minor – Disaster with RTO less than 5 hours

After Layer 1 (refer Table 1) has declared the disaster, Layer 2 shall inform designated team members using appropriate communication mechanisms and invoke the steps of the Disaster Recovery, based on the following:

- a) **Catastrophe:** If normal operations cannot be continued at the primary site and the facility is destroyed to the extent that an alternate facility at DR site must be used.
 - i. Anticipated time to restart operation at DC is more than 2 days
 - ii. Anticipated time to start operation at DR is between 12-15 hours.
 - iii. The IT set up (hardware / network / security etc.) and / or the facility could be destroyed.
 - iv. Respective teams shall be called to begin a total implementation of the Contingency Plan.
 - v. If the action plan requires the assistance of other recovery teams, those teams shall be notified via appropriate channels (email/call).
- b) **Major Disaster:** If normal operations can be continued or restarted at the primary site and an alternate facility at DR site must be used with the assistance of certain recovery teams

- i. Major Damage – Selected teams shall be called to direct restoration of normal operations at current site.
 - ii. Anticipated time to restart operation at DC is more than 5 hours but less than 2 Days.
 - iii. Anticipated time to start operation at DR is between 3 and 5 hours.
 - iv. Major damage to hardware or facility.
 - v. If limited operations can be continued at the primary site and plans can be initiated to repair or replace unusable equipment.
- c) Minor Disaster:** If normal operations can be continued at the primary site within minor disturbances in operation and repairs can be initiated as soon as possible.
- i. Minor Damage—Processing can be restarted in short time with no special recall of personnel
 - ii. Anticipated time to restart operation at DC is less than 5 hours
 - iii. Anticipated time to start operation at DR is less than 3 hours

Damage could be to hardware, software, mechanical equipment, electrical equipment, or the facility.

5. Recovery Point Objective, Recovery Time Objective and Business Impact Analysis

5.1 RPO

Recovery Point Objective, henceforth referred to as RPO represents a measure of the maximum data loss that is acceptable in the event of a failure or unavailability of the primary site.


5.2 RTO

Recovery Time Objective, henceforth referred to as RTO represents the amount of time it takes the system (DR) to recover from failure or unavailability of the primary site.

Refer Annexure I for estimated RPO & RTO for SAP and non-SAP applications considering no additional delay owing to network failure.

Annexure I – RTO and RPO

SAP Application	Respective Stake holders	Min RTO	Max RTO	RPO
ECC	HOD / SPOC	3 hours	15 hours	30 mins
CRM	HOD / SPOC	3 hours	15 hours	30 mins
EP	HOD/ SPOC	3 hours	15 hours	30 mins
APO	HOD / SPOC	3 hours	15 hours	30 mins
PO	HOD / SPOC	3 hours	15 hours	30 mins
FIORI	HOD / SPOC	3 hours	15 hours	30 mins
Web Dispature	HOD / SPOC	3 hours	15 hours	30 mins
SAP Router	HOD / SPOC	3 hours	15 hours	30 mins

Havells India Limited Havells India IT Continuity Policy Version 1.0 Internal	 HAVELLS
--	---


Non-SAP Application	Respective Stake holders	Min RTO	Max RTO	RPO
SFA	HOD / SPOC	3 hours	15 hours	30 mins
MDM	HOD / SPOC	3 hours	15 hours	30 mins
Power Plus	HOD/ SPOC	3 hours	15 hours	30 mins
Dealer Portal	HOD/ SPOC	3 hours	15 hours	30 mins
Mkonnnect	HOD / SPOC	3 hours	15 hours	30 mins
OCR	HOD / SPOC	3 hours	15 hours	30 mins
Shipment Tracking	HOD / SPOC	3 hours	15 hours	30 mins
LPMS	HOD / SPOC	3 hours	15 hours	30 mins
PMS	HOD / SPOC	3 hours	15 hours	30 mins

Infrastructure	Respective Stake holders	Min RTO	Max RTO	RPO
AWS (IaaS) Production	HOD / SPOC	30 mins	1 hour	24hrs
AWS (IaaS) Dev/QA	HOD/ SPOC	30 mins	1 hour	24hrs
AWS (RDS)	HOD/ SPOC	30 mins	3 hours	10 mins
Microsoft Azure (IaaS)	HOD/ SPOC	30 mins	2 hours	24hrs
Microsoft Azure (PaaS)	HOD/SPOC	30 mins	2 hours	24hrs
Microsoft Azure (DaaS) MS SQL	HOD/SPOC	30 mins	2 hours	2 hours
Microsoft Azure (DaaS) MS SQL	HOD/SPOC	30 mins	2 hours	1 hour

Note- Above RPO/RTO is inline to backup happening on respective cloud Infrastructure

Annexure II – BC/DR Team Telephone Numbers

Sr. No.	Name	Role	Phone Number		Email
			Office	Mobile	
1	Mr. Pramod Mundra	CIO	+91-120-477-1679 (715-1679)	+919717005106	Pramod.Mundra@havells.com
2.	Mr. Gaurav Taxali	Information Technology Head	+91-120-477-1679 (715-1678)	+919899092948	Gaurav.Taxali@havells.com
3.	Mr. Ramanand Jha	Information Security Head	+91-120-477-1679 (715-2461)	+919958644227	Ramanand.jha@havells.com
4.	Mr. Sanjay Roongta	IT Infra Lead	+91-120-477-2725 (715-2725)	+919910229944	Sanjay.Roongta@havells.com
5.	Mr. Radhashyam Sahoo	DNE Lead	+91-120-477-1642 (715-1642)	+919650666440	Radhashyam.Sahoo@havells.com

Havells India Limited Havells India IT Continuity Policy Version 1.0 Internal	
--	---


6.	Mr. Neeraj Nagpal	Information Security Lead	+91-120-477-2706 (715-2706)	+919810780536	neeraj.nagpal@havells.com
7.	Mr. Kumar Rajan	Application Lead	+91-120-477-2730 (715-2730)	+918800827252	Kumar1.Rajan@havells.com
8.	Mr. Brajesh Kumar	Basis Support Lead	+91-120-477-2717 (715-2717)	+919811591456	Brajesh1.Kumar@havells.com
9.	Hemant Bairwa	Project Lead	+91-120-477-2727 (715-2727)	+919958992322	Hemant.Bairwa@havells.com
10.	Mr. Rahul Shekhawat	Backup Team Lead	+91-120-477-2728 (715-2728)	+919871110605	rahul.shekhawat@havells.com
11.	Mr. Rahul Tyagi	End User Support Lead	+91-120-477-1338 (715-1338)	+919971625522	rahul.tyagi@havells.com

Annexure III- Havells' Head Office Escalation

Level 1	Level 2	Level 3	Level 4	Level 5
Hemant Kumar	Neeraj Nagpal	Sanjay Roongta	Gaurav Taxali (IT Head) & Ramanand Jha (Information Security Head)	Pramod Mundra (CIO)
Mobile : 9958992322	Mobile : 9810780536	Mobile : 9910229944	Mobile : +919899092948 Mobile: +919958644227	Mobile : +919717005106
Hemant.Bairwa@havells.com	neeraj.nagpal@havells.com	sanjay.roongta@havells.com	Gaurav.Taxali@havells.com RAMANAND.JHA@HAVELLS.COM	pramod.mundra@havells.com

Annexure IV- Emergency Telephone Numbers

EMERGENCY SERVICE NUMBERS			
S.NO	SERVICE NAME	CONTACT NO.	
Emergency Services			
1	POLICE CONTROL ROOM	100	
2	FIRE CONTROL ROOM	101	

<p>Havells India Limited Havells India IT Continuity Policy Version 1.0 Internal</p>	
---	---

EMERGENCY SERVICE NUMBERS			
3	AMBULANCE	102	

Annexure V- For DC Facility – Refer respective Colocation DC escalation Matrix
